Experts encourage vigilance to combat 'hacker attacks'

By Kathleen T. Rhem
American Forces Press Service

Increased tensions between America and Iraq could lead to an increase in global hacking activities, the government body dedicated to protecting the nation's infrastructure warned.

"Recent experience has shown that during a time of increased international tension, illegal cyber activity … often escalates," states a Feb. 11 advisory issued by the National Infrastructure Protection Center.

Illegal activities can include Web defacements, denial-of-service attacks and spamming.

The advisory warns the hacking activity can come from other countries that are party to the tensions, can be state sponsored or encouraged, or come from individuals or private groups.

Attacks of foreign and domestic origins may arise from political activism by those opposed to war with Iraq. They can also signal criminal activity masquerading as political activism, the advisory warns.

Other hacker attacks can come from individuals sympathetic to the U.S. government position on Iraq, "which they view as somehow contributing to the cause," the advisory states.

> *"During a time of increased international tension, illegal cyber activity often escalates."*
>
> **National Infrastructure Protection Center**
> *www.nipc.gov*

The Infrastructure Protection Center urged computer and network users to review their defenses against hacker attacks and to be increasingly vigilant in monitoring their systems. It also provided a list of "security best practices" for computer users to follow:

- Increase user awareness.
- Update anti-virus software.
- Stop suspicious attachments at the server level.
- Use filtering software to maximize security.
- Establish policies and procedures for responding to attacks and recovering data.

For more information visit the National Infrastructure Protection Center's Web site at www.nipc.gov.

This article can be accessed online at www.defenselink.mil.

FORCE PROTECTION FACTS

The following Web sites are but a few of the many force protection resources available in cyberspace:

U.S. Department of State
www.state.gov
Contains information about living and traveling abroad as well as security updates on countries and regions throughout the world.

U.S. Department of Homeland Security
www.dhs.gov
Explains the current color-coded security threat level and precautions; news alerts; an overview of DHS's mission and structure; and other information for citizens, businesses, governments and employees.

U.S. Army, Europe, Automation Training Program
https://www.uatp.hqusareur.army.mil
Features an online computer-user study guide and copy of the USAREUR computer user agreement. Also hosts the test that all must pass before being granted network access.

USAREUR Office of the Provost Marshal
www.hqusareur.army.mil/opm/opmhome.html
Offers guidance on vehicle and firearms registration, customs, terrorism prevention; provides text of regulations, pertinent links and more.

Defense Threat Reduction Agency
www.dtra.mil
Links to information on combat support; deployed military family support; technology developments relating to weapons of mass destruction; threat control and more.

Maria Higgins

Password security is an integral component of computer network security. Experts advise users to never share their passwords or store them in easily accessible locations, such as beneath a mouse pad or in an unlocked desk drawer.

Computer users responsible for keeping network secure

By Hugh C. McBride

Regardless of one's computer expertise – from newbie to techno-wiz – anyone who has access to a military computer shares in the responsibility of keeping the network secure.

Though both software protections and trained professionals work around the clock to keep the network safe, "the user is ultimately responsible for what happens on his or her machine," said Troy Hall, chairman of the 6th Area Support Group's Automation Working Group.

Hall said significant technological safeguards are in place to protect the network. However, users must ensure that they don't compromise these efforts – either intentionally or inadvertently.

For example, actions as "innocent" as using a personal digital assistant (such as a PalmPilot) at work or downloading an MP3 music file can hamper the effectiveness of the network – and are against policy unless done with appropriate approval.

The bottom line, Hall said, is that computer users need to stay aware of local policies and, if in doubt, consult with their information management officer.

"If you notice anything odd about your computer's operation," he said, "you need to notify your IMO immediately."

Computer security tips

- Never share your password with anyone.
- Limit Internet access to approved, work-related activities.
- Notify your information management officer immediately if your machine malfunctions.
- Do not install software without permission.